Formalization and closedness of finite dimensional subspaces

Florian Faissole

Formalization and closedness of finite dimensional subspaces

Florian Faissole
Inria, Université Paris-Saclay, F-91893 Palaiseau
LRI (CNRS, Univ. Paris-Sud), Université Paris-Saclay, F-91405 Orsay
Email: florian.faissole@inria.fr

***Abstract*—This article presents a Coq formalization of finite dimensional subspaces of Hilbert spaces: we prove that such subspaces are closed submodules. This result is one of the basic blocks to prove the correctness of the finite element method which approaches the solution of partial differential equations. The exact solution is valued in a continuous volume (Hilbert space) while the approximation is valued in a mesh (finite dimensional subspace) which fits the shape of the volume. When applied to a submodule which is finite dimensional, Lax–Milgram Theorem and Céa Lemma ensure the finite element method is sufficiently precise. We rely on filters as basis for topological reasoning: filters provide a very general framework to express local properties and limits. However, most such mathematical literature does not rely on filters, making our Coq formalization unusual.**

***Keywords*-formal proof; Coq; functional analysis; filters; finite dimensional subspaces; formalization of mathematics;**

I. Introduction

Finite dimensional subspaces of Hilbert spaces (a Hilbert space is a complete module endowed with an inner product) serve as foundation for the finite element method. The finite element method provides approximated solutions for some classes of Partial Differential Equations (PDEs) [11]. The Lax–Milgram Theorem is one of the main results to prove the correctness of this method, and is applied on closed submodules of Hilbert spaces. When applied to finite dimensional subspaces, it establishes existence and uniqueness of the solution of a PDE both on an infinite dimensional functional Hilbert space and on its discrete approximation (on a finite dimensional subspace) commonly solved on a mesh which fits the shape of the continuous volume. The Céa Lemma is a corollary which provides a bound on the error between the discrete approximation and the exact solution.

A proof assistant is a software tool to assist humans developing formal proofs. It comes with a specification language based on a given logical formalism (set theory, type theory ...) and a tactic language to perform proofs in an interactive way. We can mention Coq [3], HOL-Light [16], Isabelle/HOL [26] and PVS [25]. In this paper, we use Coq: it is based on a higher-order type theory with inductive types and dependent types, belonging to the family of typed lambda calculi [3]. Moreover, the logic of Coq is intuitionistic and the excluded-middle is not assumed by default (but can be used as an external axiom). Coq has been used to prove substantial results, such as the comprehensive proofs of the Odd-Order Theorem [13] and the Four Colour Theorem [12].

The Lax–Milgram Theorem and the Céa Lemma have been formalized [4] in the Coq proof assistant. To establish the soundness of the finite element method and to verify programs implementing the method, one needs to apply the Lax–Milgram Theorem both on a Hilbert space E and on a finite dimensional subspace of E. We have to prove such a finite dimensional subspace is a closed submodule.

There has been growing interest within the interactive theorem proving community in formalizing analysis, which serves as foundation for critical applications, such as resolution of differential equations for aeronautics or medicine. There are several examples of formalization of finite dimensional vector spaces or modules both in HOL-Light [15], in Isabelle/HOL [10] and in Coq [8], [13]: for instance, in the Mathematical Component library, finite dimensional vector spaces are defined as a canonical structure [22] and serve in the proof of the Odd-Order Theorem [13]. Works by Harrison [15] and Brunel [8] are more precisely focused on Euclidean spaces, $i.e.$ finite dimensional Hilbert spaces. In particular, Brunel defines the space $\mathbb{R}^n$ by induction on n and then uses a typeclass to endow $\mathbb{R}^n$ with an inner product and its axiomatic properties [8]. Harrison does not put the dimension of the space as an argument of the type, but uses a type A of cardinal n: hence the functional type $A \to \mathbb{R}$ represents $\mathbb{R}^n$ [15]. Actually, a type of cardinal n is a type inhabited by n elements and one can for instance take $A = Unit + \ldots + Unit$ (n times).

In these developments, finite dimensional spaces are defined as first-class citizens and one can consider smaller finite dimensional subspaces of these spaces. When considering a finite dimensional underlying Euclidean space E of dimension n and spanning family B, one can characterize a finite dimensional subspace φ of E by a sub-family of elements of B and a restriction of the inner product. Hence some properties (closedness, completeness, ...) of the subspace can be derive easily from the properties of E. In our work, the underlying space is possibly infinite, making the proofs more complex. It will serve to discretize complex continuous volumes by finite dimensional meshes. Nevertheless, we can mention the work of Afshar, Aravantinos, Hasan and Tahar [1] and the work of Mahmoud, Aravantinos and Tahar [23] both in Isabelle/HOL: they define both

finite dimensional and infinite dimensional vector spaces of complex numbers but they do not work in general Hilbert spaces.

Our formalization relies on the Coquelicot library [5], [20], [21], a conservative extension of the Coq standard library of real numbers [24] based on general topology. We provide a formal definition of finite dimensional subspaces of Hilbert spaces and prove that they are submodules. Closedness is more challenging both from mathematical and formalization standpoints. In general, proving that a finite dimensional subspace of a complete space is closed relies on compactness properties [14, Th 6.28 pp. 192–3]. To overcome this difficulty, we rely on a detailed pen-and-paper proof written by Clément and Martin [9], which is valid in Hilbert spaces and does not use compactness. However, this detailed proof uses sequences of elements of Hilbert spaces: Clément and Martin more precisely study the behavior of sequences built from other ones in topological reasonings. As the Coquelicot library provides very general outcomes for topology [20], filters are used instead of sequences: filters are a generalization of neighborhoods and could be defined on any topological space without metric or norm [6] (see Section II). That is why we cannot directly translate the paper proof [9] in Coq and have to build suitable filters and filters transformers whenever sequences are used.

In most of the mathematical literature (see for instance [7]), functional analysis assumes at least weak variants of the choice axiom [18]. Although constructive functional analysis has been studied [28], it is built upon mathematical foundations very different from those in which the finite element method is built. In the Coq proof of the Lax–Milgram Theorem [4], full classical logic is not assumed, but axioms from the Coq real standard library are used, and some decidability hypotheses are injected at some points. In the closedness proof of finite dimensional subspaces we want to formalize, the use of classical logic is even more frequent (not because of the structure of the finite dimensional subspace but rather because of the overlying Hilbert space). That is why our choice is to assume the law of excluded-middle for readability. In this article, we do not provide all the details of the proofs but we want to give an intuition of the interesting points of the reasoning. The Coq code is available at the following address:

https://github.com/FFaissole/FDIM_Topology.

The main theorem we formally proved in this article can be stated as:

Theorem. *Let $E : Hilbert$ and $F \subseteq E$.*
Suppose F is finite dimensional with dimension n and orthonormal spanning family B. Then F is closed.

Sketch of the proof: The linear span of a vector $u \in E$: $Hilbert$ is a closed subset of E. It follows that the direct sum of a closed subspace and the linear span of u is closed (1). Actually, a finite dimensional subspace of dimension n is a direct sum of another finite dimensional subspace of dimension $n-1$ and the linear span of a vector (2). We reason by induction and suppose that finite dimensional subspaces of dimension $n-1$ are closed. Using (1) and (2), we conclude that a finite dimensional subspace is closed.

Plan: Section II presents the background we rely on, more precisely filters and the way they are implemented in the Coquelicot library. Section III describes our formalization of finite dimensional subspaces together with the proofs of preliminary properties. Section IV is dedicated to the linear span of vectors and the proof of its closedness under few assumptions. The orthogonal projection of a vector on a closed subset is described in Section V, where its continuity is proved. In Section VI, we prove that finite dimensional subspaces of Hilbert spaces are closed. Finally, Section VII concludes our work and suggests some perspectives.

II. General topology and Coquelicot library

General topology provides structures to define notions of neighborhoods, continuity and convergence in topological spaces. There are several ways to define limits and one of the more powerful uses the formalism of filters. This section presents basic facts about filters and the way they are formalized in the Coquelicot library [5].

A. Filters

Filters are a generalization of neighborhoods, more precisely sets of neighborhoods with a few assumptions given below. A collection $\mathcal{F} : (E \to Prop) \to Prop$ ($Prop$ the type of propositions) of subsets of E is a filter if it verifies:

1) $\emptyset \notin \mathcal{F}$;
2) if $U \in \mathcal{F}$ and $V \in \mathcal{F}$ then $U \cap V \in \mathcal{F}$;
3) if $U \in \mathcal{F}$ and $U \subseteq V$ then $V \in \mathcal{F}$.

Some examples of simple filters can be seen in Figure 1. Topological notions involving sequences can be defined in a similar way with filters, such as convergence, Cauchy's property, continuity, completeness or closedness.

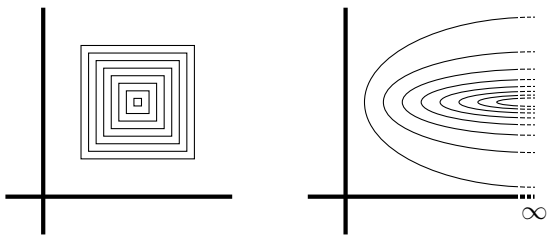

Figure 1. Example of filters, toward: a finite point (left), infinity (right).

B. Coquelicot: a library using filters

Coquelicot is a Coq library for real analysis with original features [5], [20], [21]. First, it uses total functions for limits and thus for derivative and integrals. Moreover, it comes with a general hierarchy of spaces based on

canonical structures [22]. Thus, we can reason on algebraic structures such as groups or on topological spaces (seen as types) which are not necessarily endowed with a metric or a norm. The machinery of filters for the formalization of analysis in proof assistants has been initiated by Hölz, Immler and Traut in the Isabelle/HOL system [17]. Following similar ideas, the Coquelicot topology is defined using filters. For instance, the filter `eventually` on type `nat` is used to define the convergence of sequences:

```
Definition eventually (P:nat → Prop) :=
    ∃ N, ∀ n, (n ≤ N) → P n.
```

A uniform space is any type endowed with a kind of metric defined by a predicate `ball` between two elements and a real number (`ball x e y` intuitively means that the distance between `x` and `y` is smaller than `e`) and its axioms. The `locally` filter defines the neighborhoods of $x \in U$ with U uniform space:

```
Definition locally (P:U → Prop) (x:U) :=
    ∃ eps : posreal,
      ∀ y:U, ball x eps y → P y.
```

To give an intuition of this filter, as stated in [5],

$$locally(P, x) \Leftrightarrow \exists \varepsilon > 0, \forall u \in U, |x - u| < \varepsilon \Rightarrow P(u).$$

In Coquelicot, a filter is said to be a proper filter (`ProperFilter`) if it only contains inhabited elements. A Cauchy filter (`cauchy`) is a filter which contains arbitrarily small balls (it corresponds to a generalization of Cauchy sequences):

```
Definition cauchy {T:UniformSpace}
(F:(T→Prop)→Prop) :=
     ∀ eps : posreal, ∃ x, F (ball x eps).
```

A complete space `T` is a uniform space with a limit function and its property.[1] The function is `lim : ((T → Prop) → Prop) → T`: it takes a filter on `T` and returns an element of `T` (the limit of the filter). The completeness property expresses the convergence of any proper and Cauchy filter on `T`:

```
∀ F, ProperFilter F → cauchy F →
     ∀ eps, F (ball (lim F) eps).
```

Intuitively, it means that an inhabited filter containing arbitrary small balls also contains arbitrary small balls whose center is the limit of the filter. The function `lim` is actually a total function and maps non-convergent filters to a given value which does not matter.

[1]In the latest version of the Coquelicot library (coquelicot 3.0.0), the definition has changed and is enriched by another axiom.

One can also define the image of a filter by a given function. It generalizes the construction of a sequence $f(u_n)$ from a sequence u_n and a function f. The Coquelicot's operator `filtermap` maps a filter to its image by a given function:

```
Definition filtermap {T U : Type}
   (f:T→U) (F:(T → Prop) → Prop) :=
        fun P ⇒ F(fun x ⇒ P (f x)).
```

It is used to define the continuity of a function between uniform spaces:

```
Definition continuous
   {T U:UniformSpace} (f:T → U) (x:T):=
      ∀ P : U → Prop, (locally (f x)) P
         → (filtermap f (locally x)) P.
```

This definition generalizes the definition of continuity which says that a function f is continuous in a point x if and only if the inverse image of every neighborhood of $f(x)$ is also a neighborhood of x. Continuous functions have an interesting property: if a filter converges towards a given limit ℓ, the image of this filter by a continuous function f converges towards the image $f(\ell)$ of the limit. This last property is central in the closedness proof of finite dimensional subspaces we provide below. Indeed, we build the image of filters by continuous functions and we need to extract their limits.

A subspace of a space E is defined by predicate φ of type $E \to Prop$ (for more readability in this paper, we use both notations $\varphi(u)$ and $u \in \varphi$ for the membership of an element $u \in E$ to a subspace φ of E). Without dependent types, it is not possible to say that a filter is a filter on φ, as it can only have type $(E \to Prop) \to Prop$ (and thus it is a filter on E). Nonetheless, we can "link" a filter on E with a subspace φ by the following definition:

Definition 1. *Let $E : Type$. Let $\mathcal{F} : (E \to Prop) \to Prop$ a filter on E.*
Let $\varphi : E \to Prop$ a subspace of E. $\mathcal{F}$ is implicitly a filter on φ if:

$$\forall \psi : E \to Prop, \mathcal{F}(\psi) \Rightarrow \exists x \in E, \psi(x) \wedge \varphi(x).$$

It means that the filter only contains subsets which have an inhabited intersection with φ. A subset φ of $E : CompleteSpace$ is closed if for any proper Cauchy filter $\mathcal{F}$ implicitly on φ, the limit of $\mathcal{F}$ is in φ:

Definition 2. *Let $E : CompleteSpace$, $\varphi : E \to Prop$. The subset φ is closed in E iff forall filter $\mathcal{F} : (E \to Prop) \to Prop$, if $\mathcal{F}$ is proper, cauchy and implicitly on φ then $lim(\mathcal{F}) \in \varphi$.*

III. Finite dimensional subspaces

In Section III-A, we consider a subspace of E and we define the property of being finite dimensional for this

subspace. Then, in Section III-B, we prove that finite dimensional subspaces are submodules.

A. Definitions

Suppose that $E : Hilbert$ (complete module with an inner product and the associated axioms [4]). We say a subspace is finite dimensional (of dimension n) if it verifies the property `FDIM`: there exists a spanning family of vectors B whose cardinal is at most equal to n. In the following Coq code, (`sum_n f n` is the sum of the $f(i)$ for $0 \leq i \leq n$ and `scal` is the multiplication by a scalar).

```
Variables (E:Hilbert)(n:nat)(B:nat→E).

Definition FDIM (phi:E → Prop) :=
   match (eq_nat_dec n 0) with
    |left _ ⇒ ∀ u, phi u ↔ u=zero (* n=0 *)
    |right _ ⇒ ∀ u, phi u ↔ (* n>0 *)
      ∃ L:nat → R, u = sum_n (fun i ⇒
          scal (L i) (B i)) (n-1) end.
```

Spanning family: Our standpoint is to define B as a sequence and not as a list of length n. Thus, for $M \geq n$, the value of $B(M)$ does not matter.

Overestimation of the dimension: Similarly, n does not correspond to the strict definition of the dimension of a finite dimensional subspace. Indeed, let us imagine, for $M < n$, that $B(M) = 0$. Hence n is an overestimation of the dimension of the subspace, but it does not affect the proofs and gives us more flexibility.

Orthonormality of the spanning family: We define the orthonormality of B (`inner` is the inner product):

```
Definition B_ortho (B : nat → E) :=
    ∀ (i:nat), (inner (B i) (B i)) = 1
     ∧ (∀ i j, i ≠ j
       → (inner (B i) (B j)) = 0).
```

Assuming that B is orthonormal is a way to simplify the reasoning without loss of generality. Actually, the Gram-Schmidt algorithm is a canonical way to transform any spanning family into an orthonormal one [19]. It is crucial in the final step of the proof of closedness in Section VI.

B. ModuleSpace-compatibility

Definition 3. *A subset φ of $E : Hilbert$ is `ModuleSpace`-compatible iff:*

1) $\varphi(0)$;
2) $\forall x \in E, y \in E, \varphi(x) \Rightarrow \varphi(y) \Rightarrow \varphi(x - y)$;
3) $\forall x \in E, \lambda \in \mathbb{R}, \varphi(x) \Rightarrow \varphi(\lambda x)$.

The first condition needed to apply the Lax–Milgram Theorem on a subspace φ of $E : Hilbert$ is to verify that φ is `ModuleSpace`-compatible.

Lemma 1. *Let $E : Hilbert$. Let $\varphi : E \to Prop$. Suppose that φ is finite dimensional. Then φ is `ModuleSpace`-compatible.*

As expected, the proof is not difficult and we just apply properties of the `sum_n` operator provided by the Coquelicot library.

IV. Linear span

After rather easy results, let us consider topological outcomes. In this section, we define the linear span of $u \in E$ ($E : Hilbert$) as the subset of vectors of E collinear to u, and we prove an intermediate theorem, which states the closedness of the linear span of any element of a Hilbert space.

```
Definition span (u : E) := fun x:E ⇒
       (∃ (l : R), x = scal l u).
```

In their proof, Clément and Martin manipulate sequences valued in the subspace $span(u)$ of E [9]. Such sequences are of the form $(\lambda_n u)_{n\in\mathbb{N}}$ and extracting the associated real sequence $(\lambda_n)_{n\in\mathbb{N}}$ is immediate. As we are working with filters, we want to extract a filter on $\mathbb{R}$ from a filter on E.

Although one can say that a sequence is valued in a subset φ of E (for example in $span(u)$), we can just say that a filter is implicitly on φ (see Section II-B). That is why we define filter transformers as total functions: for instance, if one wants to simulate the transformation $(u_n)_{n\in\mathbb{N}} \to (v_n)_{n\in\mathbb{N}}$ (where $(u_n)_{n\in\mathbb{N}}$ and $(v_n)_{n\in\mathbb{N}}$ are valued respectively in E_1 and E_2) from the standpoint of filters, one has to define a total function from filters on E_1 to filters on E_2. To simulate the transformation $(\lambda_n u)_{n\in\mathbb{N}} \to (\lambda_n)_{n\in\mathbb{N}}$ with filters, we define an operator which maps a filter $\mathcal{F} : (E \to Prop) \to Prop$ to a filter of type $(\mathbb{R} \to Prop) \to Prop$:

```
Definition clean_scal (u : E)
  (F:(E→Prop)→Prop):(R →Prop)→Prop
     := fun A:(R → Prop) ⇒ ∃ V:E → Prop,
        F V ∧ ( ∀ l, V (scal l u) → A l).
```

It is a total function. It is defined on any filter $\mathcal{F}$ of E, but we are mainly interested in the case where $\mathcal{F}$ is implicitly on $span(u)$. In this case, `clean_scal` generalizes the sequence transformer $(\lambda_n u)_{n\in\mathbb{N}} \to (\lambda_n)_{n\in\mathbb{N}}$. To use the properties of the extracted filter, it is necessary to prove relations between the source and the target filters. Actually, if the source filter is a proper and Cauchy one, the image filter has the same properties.

Lemma 2. *Let $E : Hilbert$, $u \in E$ ($u \neq 0$) and $\mathcal{F} : (E \to Prop) \to Prop$. Suppose that $\mathcal{F}$ is a proper Cauchy filter implicitly on $span(u)$.*
Then $clean\_scal(u, \mathcal{F})$ is a proper and Cauchy filter on $\mathbb{R}$.

The Cauchy property is the most interesting: we know that the source filter contains arbitrary small balls and thus we have to find arbitrary small balls in the target filter. The reasoning involve manipulation of balls, and hence we have to use several properties of uniform spaces.

From all the previous results, let us prove that the linear span of a vector $u \in E$ is a closed subset of E.

Theorem 3. *Suppose E : Hilbert, $u \in E$. Then $span(u)$ is closed in E.*

Proof: The proof of this theorem requires to distinguish the case where $u = 0$: in this case, $span(u) = \{0\}$ and we know every singleton subset is closed, and thus $span(u)$ is closed. When $u \neq 0$, let us consider a proper Cauchy filter $\mathcal{F}$ implicitly on $span(u)$. In this case, we know by Lemma 2 that the filter $clean\_scal(u, \mathcal{F})$ on $\mathbb{R}$ is a Cauchy filter. We know that $\mathbb{R}$ is complete and thus that $clean\_scal(u, \mathcal{F})$ has a limit ℓ such that $\forall \varepsilon$, $(ball\ \ell\ \varepsilon) \in clean\_scal(u, \mathcal{F})$.

Thus, as E is complete, every Cauchy filter on E has a unique limit, and we show that if $clean\_scal(u, \mathcal{F})$ has limit ℓ, $\mathcal{F}$ has limit ℓu, which is obviously in $span(u)$. Thus $span(u)$ is closed (see Definition in Section II-B). ■

V. About the orthogonal projection

Some existing paper proofs of closedness of finite dimensional subspaces, such as the one by Clément and Martin [9], involve sequences built as image of other ones by orthogonal projectors. Hence we want to build images of filters by the same projectors, and to be able to derive easily the limits of these image filters. That is why we want to prove the continuity of the projectors.

The orthogonal projection of a vector u on a subspace φ is the vector $proj_\varphi(u)$ which verifies the following properties:

$$proj_\varphi(u) \in \varphi \wedge \forall v \in E, \|u - proj_\varphi(u)\| = \min_{v \in \varphi} \|u - v\|$$

In the formalization of the Lax–Milgram Theorem [4], there is a characterization of the orthogonal projection of a vector on a subspace by its properties (described just above). However, the development [4] does not provide the orthogonal projection as a function taking a vector and a subspace. To build the function mapping an element to its orthogonal projection on a subspace φ, we use Coquelicot's `iota` operator (below `Glb_Rbar P` is the infimum of the subspace `P` of type $\overline{\mathbb{R}} \to$ `Prop`) :

```
Definition proj (phi:E → Prop) :=
  fun u:E ⇒ iota (fun v:E ⇒ phi v ∧
    norm (minus u v) = Glb_Rbar (fun r ⇒
     ∃ w:E, phi w ∧ r = norm (minus u w))).
```

We prove that if $u \in \varphi$, the orthogonal projection $proj_\varphi(u)$ of u on φ is equal to u. In contrast, if u is in the orthogonal complement $\varphi^\perp$ of φ ($\varphi^\perp = \lambda z : E\ .\ \forall x, x \in \varphi \Rightarrow \langle x, z\rangle = 0$), $proj_\varphi(u) = 0$. We also prove that:

$$\forall x, y \in E, \|proj_\varphi(x) - proj_\varphi(y)\| \leq \|x - y\|.$$

A. Linearity

We derive the linearity of the orthogonal projection:

Lemma 4. *Let E : Hilbert and $\varphi : E \to Prop$ closed. Let $x, y \in E, \lambda \in \mathbb{R}$. Then, $proj_\varphi(x-y) = proj_\varphi(x) - proj_\varphi(y)$ and $proj_\varphi(\lambda x) = \lambda proj_\varphi(x)$.*

Proof: Even if the linearity of $proj$ is graphically well-understood, the formal proof is tricky because of the manipulation of the greatest lower bound `Glb_Rbar` (which is valued in $\overline{\mathbb{R}}$) and the `iota` operator. Moreover, we need to state the existence of the orthogonal projection for each manipulated vector (x, y, λx, $x - y$) using the existence and uniqueness lemma. ■

B. Continuity

Together with the linearity, another interesting property of the orthogonal projection map is its continuity, as defined in Section II-B. Clément and Martin use a sequence $(u_n)_{n\in\mathbb{N}}$ and refer to the sequences $(proj_\varphi(u_n))_{n\in\mathbb{N}}$ and $(proj_\varphi(u_n) - u_n)_{n\in\mathbb{N}}$ [9]. Thus, we have to build the corresponding filters: we define two operators $clean\_proj$ and $clean\_proj'$ which transform a given filter into their projections:

```
Definition clean_proj (phi:E → Prop)
   (F:(E→Prop)→Prop)): (E→Prop)→Prop
       := filtermap (proj phi) F.
Definition clean_proj' (phi:E → Prop)
   (F:(E→Prop)→Prop)): (E→Prop)→Prop
 := filtermap (fun u ⇒ u - proj phi u) F.
```

We first prove that the images of a proper Cauchy filter on E by `clean_proj` and `clean_proj'` are proper and Cauchy on E to perform the proof of the following lemma:

Lemma 5. *Suppose E : Hilbert and $\varphi : E \to Prop$. Then $proj_\varphi$ and $x \mapsto x - proj_\varphi(x)$ are continuous.*

VI. Closedness properties

Finally, we discuss the closedness of finite dimensional subspaces of Hilbert spaces. In Section VI-A, we show that the direct sum of a closed subspace and a linear span is closed. In Section VI-B, we show that a finite dimensional subspace of dimension n is actually a direct sum of another finite dimensional subspace of dimension $n-1$ and the linear span of an element of the spanning family. By induction, we conclude that a finite dimensional subspace is closed.

A. Direct sum and closedness

Direct sum of subspaces of modules is an important notion in the theory of Hilbert spaces. It is a way to decompose spaces into simpler ones and thus to decompose problems we want to solve on these spaces.

Definition 4. *Let $E : Hilbert$, $\varphi, \psi, \pi : E \to Prop$. We say that $\varphi = \psi \oplus \pi$ (φ is the direct sum of ψ and π) iff:*

$$\forall u \in E, \varphi(u) \Rightarrow \exists! a, b \in E, a \in \psi \wedge b \in \pi \wedge u = a + b$$

We prove that the direct sum of a closed subset and a linear span is closed:

Theorem 6. *Let $E : Hilbert$, $\varphi, \psi : E \to Prop$, $u \in E$. Suppose that ψ closed, $\varphi = \psi \oplus span(u)$ and $u \in \psi^\perp$. Then φ is closed.*

Let us focus on the use of the two operators $clean\_proj$ and $clean\_proj'$ to decompose any Cauchy filter implicitly on $\varphi = \psi \oplus span(u)$ into two filters. The first one is $clean\_proj_\psi$: it maps a filter implicitly on φ on a filter implicitly on ψ. We show that the second one ($clean\_proj'_\psi$) maps to a filter implicitly on $span(u)$ (which is a non-trivial consequence of the fact that $u \in \psi^\perp$). We use properties of direct sums previously formalized in Coq [4] and the closedness of $span(u)$ provided by Theorem 3.

The proof also requires limits for $clean\_proj_\psi(\mathcal{F})$ and $clean\_proj'_\psi(\mathcal{F})$. As we know $proj_\psi$ and $x \mapsto x - proj_\psi(x)$ are continuous by Lemma 5, if $\mathcal{F}$ has limit ℓ, $clean\_proj_\psi(\mathcal{F})$ and $clean\_proj'_\psi(\mathcal{F})$ have limits $proj_\psi(\ell)$ and $\ell - proj_\psi(\ell)$.

B. Closedness of finite dimensional subspaces

Theorem 7. *Let $E : Hilbert$ and $\varphi : E \to Prop$. Suppose φ is finite dimensional with dimension n and orthonormal spanning family B. Then φ is closed.*

Proof: We reason by induction on n:

- $n = 0$: in this case, $\varphi = \{0\}$. We know every singleton subset is closed, and thus φ is closed.
- $n = N + 1$: as φ is finite dimensional:

  $$\forall u \in \varphi, \exists L : \mathbb{N} \to \mathbb{R}, u = \sum_{i=0}^{N} L_i B_i = \sum_{i=0}^{N-1} L_i B_i + L_N B_N$$

  Moreover, because of the orthogonality of B, this decomposition is unique, and thus:

  $$\exists \psi : E \to Prop, \varphi = \psi \oplus span(B_N).$$

  and ψ is finite dimensional with dimension N and spanning family $B_\psi = B$.
  By induction hypothesis, ψ closed as B_ψ is also orthogonal. Moreover, as B is orthogonal, $B_N \in \psi^\perp$.
  Thus, by Theorem 6, $\varphi = \psi \oplus span(B_N)$ is closed.

■

VII. Conclusion and Perspectives

The formal proofs of the `ModuleSpace`-compatibility and the closedness of the finite dimensional subspaces of Hilbert spaces are achieved. Our development is more than 1500-lines long, which is bigger than the existing pen-and-paper proofs, even the most detailed ones [9] (about 3 pages). The authors of the Coq proof of the Lax–Milgram Theorem [4] make a different observation: the formal proof is comparable in magnitude with the detailed pen-and-paper proof [9] (about 8000 lines of Coq for 50 pages of pen-and-paper proof). Our particularity mainly arises from the purely topological nature of the outcomes we are interested in and thus the intensive use of filters. More particularly, we have to consider filter transformers, which lead us to technical choice: we consider filter transformer as total functions and thus use these functions on filters that are implicitly on a suitable subset. Furthermore, we have to deal with the use of sub-structures, which is known to be difficult in Coq.

Our formal proof is classical and assumes the law of excluded-middle. However, as we use the real numbers from the Coq real standard library [24], the limited principle of omniscience (LPO) should be derived [5]. It allows us to get decidability of a large class of properties: for instance, we can prove that the membership of a vector to a finite dimensional subspace of a Hilbert space is decidable. Actually, it is possible to isolate a set of decidability hypotheses instead of invoking full classical logic: an alternative version of the Coq code without classical logic is available online.[2]

One of the finalities of our finite dimensional subspaces is to apply the Lax–Milgram Theorem and the Céa Lemma on these subspaces. The correctness of the finite element method requires more mathematical background. Indeed, we have to consider particular cases of Hilbert functional spaces, and thus particular finite dimensional subspaces. Some Sobolev spaces, such as $L^2(\Omega)$ or $H^1(\Omega)$ and $H^1_0(\Omega)$ (for Ω a bounded and regular domain of $\mathbb{R}^d$ with $d = 1$, 2, or 3), are interesting in this context. They are known to be Hilbertian, but a formal proof of this property seems challenging. The formalization of interpolation and meshes theory is another interesting perspective. Meshes have to be formalized in a way they could be considered as particular case of finite dimensional subspaces of a Hilbert space as defined in the present article.

Actually, the correctness of the finite element method, and more precisely the convergence property, is crucial to verify programs intended to numerically solve partial differential equations, such as the FELiScE[3] library written in C++. Furthermore, the finite element method has been implemented in symbolic computation software such as Matlab [2] and Mathematica [27]. Such formal verification could improve confidence in the Finite Element Method and in critical software numerically solving partial differential equations.

Acknowledgment

We are grateful to Sylvie Boldo for fruitful discussions about the presentation of this article. We are grateful to François Clément, Vincent Martin, and Micaela Mayero for

[2] https://github.com/FFaissole/FDIM_Topology

[3] Finite Elements for Life Sciences and Engineering https://gforge.inria.fr/projects/felisce/

discussions about the pen-and-paper proofs of topological outcomes and the formalization of filters in Coq.

REFERENCES

[1] S. K. Afshar, V. Aravantinos, O. Hasan, and S. Tahar. Formalization of complex vectors in higher-order logic. *CoRR*, abs/1405.4034, 2014.

[2] J. Alberty, C. Carstensen, S. A Funken, and R. Klose. Matlab implementation of the finite element method in elasticity. *Computing*, 69(3):239–263, 2002.

[3] Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development - Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[4] S. Boldo, F. Clément, F. Faissole, V. Martin, and M. Mayero. A Coq Formal Proof of the Lax–Milgram theorem. In *6th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 79–89, Paris, France, January 2017.

[5] S. Boldo, C. Lelay, and G. Melquiond. Coquelicot: A user-friendly library of real analysis for Coq. *Mathematics in Computer Science*, 9(1):41–62, 2015.

[6] N. Bourbaki. *Topologie générale: Chapitres 1 à 4*. Bourbaki, Nicolas. Springer Berlin Heidelberg, 1971.

[7] H. Brézis, P. G. Ciarlet, and J. L. Lions. *Analyse fonctionnelle: théorie et applications*. Collection Mathématiques appliquées pour la maîtrise. Dunod, 1999.

[8] A. Brunel. Non-constructive complex analysis in Coq. In *18th International Workshop on Types for Proofs and Programs, TYPES 2011, September 8-11, 2011, Bergen, Norway*, pages 1–15, 2011.

[9] F. Clément and V. Martin. The Lax-Milgram Theorem. A detailed proof to be formalized in Coq. Research Report RR-8934, Inria Paris, July 2016.

[10] J. Divasón Mallagaray. *Formalisation and execution of Linear Algebra: theorems and algorithms*. PhD thesis, Universidad de La Rioja, 2016.

[11] A. Ern and J. L. Guermond. *Theory and practice of finite elements*, volume 159 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 2004.

[12] G. Gonthier. *The Four Colour Theorem: Engineering of a Formal Proof*, pages 333–333. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[13] G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. Ould Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi, and L. Théry. A machine-checked proof of the odd order theorem. In *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, pages 163–179, 2013.

[14] B. Gostiaux. *Cours de mathématiques spéciales - Tome 2*. Mathématiques. Presses Universitaires de France, Paris, 1993. Topologie, analyse réelle.

[15] J. Harrison. A HOL theory of Euclidean space. In Joe Hurd and Tom Melham, editors, *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005*, volume 3603 of *Lecture Notes in Computer Science*, Oxford, UK, 2005. Springer-Verlag.

[16] J. Harrison. HOL light: An overview. In *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings*, pages 60–66, 2009.

[17] J. Hölzl, F. Immler, and B. Huffman. Type classes and filters for mathematical analysis in Isabelle/HOL. In *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, pages 279–294, 2013.

[18] P. Howard and J. E. Rubin. *Consequences of the Axiom of Choice*. Number v. 1. American Mathematical Society, 1998.

[19] D. E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. 1997.

[20] C. Lelay. How to express convergence for analysis in Coq. In *The 7th Coq Workshop*, Sophia Antipolis, France, June 2015.

[21] C. Lelay. *Repenser la bibliothèque réelle de Coq : vers une formalisation de l'analyse classique mieux adaptée*. Thèse de doctorat, Université Paris-Sud, June 2015.

[22] A. Mahboubi and E. Tassi. Canonical structures for the working Coq user. In *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, pages 19–34, 2013.

[23] M. Y. Mahmoud, V. Aravantinos, and S. Tahar. Formalization of infinite dimension linear spaces with application to quantum theory. In *NASA Formal Methods, 5th International Symposium, NFM 2013, Moffett Field, CA, USA, May 14-16, 2013. Proceedings*, pages 413–427, 2013.

[24] M. Mayero. *Formalisation et automatisation de preuves en analyses réelle et numérique*. PhD thesis, Université Paris VI, décembre 2001.

[25] S. Owre, J. M. Rushby, and N. Shankar. PVS: A prototype verification system. In *Automated Deduction - CADE-11, 11th International Conference on Automated Deduction, Saratoga Springs, NY, USA, June 15-18, 1992, Proceedings*, pages 748–752, 1992.

[26] L. C. Paulson. The foundation of a generic theorem prover. *J. Autom. Reasoning*, 5(3):363–397, 1989.

[27] C. J. Purcell. Building finite element models with mathematica. In *Mathematica Developer Conference*, 1997.

[28] B. Spitters. *Constructive and intuitionistic integration theory and function al analysis*. PhD thesis, University of Nijmegen, 2002.